[PDF] Secure link state routing for **mobile** ad hoc networks
P Papadimitratos, ZJ Haas - Proc. IEEE Workshop on Security and ..., 2003 - Citeseer
... Clearly, SLSP nodes should be able to perform **public key** operations. ... First, nodes reduce or increase their LSU **broadcast** period according to the network conditions. ... 4. Conclusions and future work We proposed a secure link state protocol (SLSP) for **mobile** ad hoc networks. ...
Cited by 174 - Related articles - View as HTML - All 16 versions

[PDF] Secure routing for **mobile** ad hoc networks
P Papadimitratos, ZJ Haas - SCS Communication Networks and ..., 2002 - Citeseer
... Abstract The emergence of the **Mobile** Ad Hoc Networking (MANET) technology advocates self-organized ... could be instantiated, for example, by the knowledge of the **public key** of the ... Finally, the **broadcast** nature of the **radio** channel mandates that each transmission is received ...
Cited by 1046 - Related articles - View as HTML - All 52 versions

ANODR: anonymous on demand routing with untraceable routes for **mobile** ad-hoc networks
J Kong, X Hong - ... of the 4th ACM international symposium on Mobile ..., 2003 - portal.acm.org
... The first one is a naive porting of MIX-Net to **mobile** ad hoc networks. ... Compared to ANODR-PO, ANODR-BO ensures that no **public key** operation is executed during RREQ ... 3 shows the case where anonymous route discovery depends completely on local **broadcast** with trap ...
Cited by 315 - Related articles - All 27 versions

Secure **broadcasting** using the secure lock
GH Chiou, WT Chen - IEEE Transactions on Software ..., 1989 - ieeexplore.ieee.org
... In this paper, we propose the concept of a secure broad- casting, effected by means of a secure lock, on **broadcast** channels, such as satellite, **radio**, etc. ... By using the secure lock, we also present protocols for secure **broadcasting**, based on the **public- key** cryptosystem as ...
Cited by 209 - Related articles - All 11 versions

Pre-loaded key based multicast and **broadcast** authentication in **mobile** ad-hoc networks
M Ramkumar, N Memon - IEEE Global Telecommunications ..., 2003 - ieeexplore.ieee.org
... communication between nodes is very crucial [6]. In general, the types of communication between various nodes may be classified as unicast, multicast and **broadcast**. ... 2) No asymmetric crypto primitives due to resource con- straints in **mobile** nodes. ... **public key** cryptography. ...
Cited by 33 - Related articles - All 6 versions

[PDF] The TESLA **broadcast** authentication protocol
A Perrig, R Canetti, JD Tygar, D Song - RSA CryptoBytes, 2002 - Citeseer
... Examples of **broadcast** distribution networks are satellite broadcasts, wireless **radio broadcast**, or IP multicast. ... TESLA is used in a wide variety of applications, ranging from **broadcast** authentication in sensor ... signature key pair, with the private key K −1 S and the **public key** K S ...
Cited by 428 - Related articles - View as HTML - All 31 versions

Mobile wireless computing: challenges in data management
T Imielinski, BR Badrinath - Communications of the ACM, 1994 - portal.acm.org

... What is the role of a wireless medium in distribution of information? How can one query data that is **broadcast** over the wireless? ... These are special **mobile radio** net- works provided by private service providers such as RAM and ARDIS. ...
Cited by 584 - Related articles - BL Direct - All 6 versions

[PDF] Secret key agreement by public discussion from common information
UM Maurer ... - IEEE Transactions on Information Theory, 1993 - Citeseer
... For instance the security of the well-known RSA **public-key** cryptosystem 11] is based on the (unproven) di ... acquire random variables X and Y is to receive the signal of a satellite **broadcasting** random bits ... avoid at least a small bit error probability), or of a deep space **radio** source ...
Cited by 565 - Related articles - View as HTML - BL Direct - All 23 versions

Mobile ip
CE Perkins - International Journal of Communication ..., 1998 - interscience.wiley.com
... **Radio** links (especially telephone) and infrared links seem to be among the most popular, but satellite systems ... busy to serve new **mobile** nodes sets the 'B' bit, but continues to **broadcast** advertisements periodically so that current registered **mobile** nodes (customers ...
Cited by 871 - Related articles - BL Direct - All 60 versions

Proactive **public key** and signature systems
A Herzberg, M Jakobsson, S Jarecki, H ... - Proceedings of the ..., 1997 - portal.acm.org
... work cleals with the general theory of proactive memory maintenance and computation in the presence of **mobile** faults in ... (Note that, here we assume **broadcast**. ... the model of [HJKY], where proactive secret sharing was illtrodrlceel and we adopt it to proactive **public key** systems. ...
Cited by 220 - Related articles - All 11 versions

[CITATION] Minimization of Boolean functions
EJ McCluskey - Bell System Technical Journal, 1956 - citeulike.org
... stream-cipher, 5. vickrey, 5. hierarchy, 5. **broadcast**, 4. random-oracle, 4. traversal, 4. inverted-hash-tree, 4. ... combinatorics, 2. stream, 2. time-stamping, 2. **mobile**, 2. one-way-trapdoor, 2. file-import-08-07-28, 2. ... set-theory, 1. factorization, 1. time-memory-data, 1. **public-key**, 1. rekey, ...
Cited by 666 - Related articles - Cached

[PDF] Providing robust and ubiquitous security support for **mobile** ad-hoc networks
H Luo, J Kong, P Zerfos, S Lu, L Zhang - IEEE ICNP, 2001 - Citeseer
... n may be dynamically changing as **mobile** nodes join, leave, or fail over time. ... (1) The **public key** PK for ... than in their wired counterpart [34], monitoring and detecting misbehav- iors among one-hop neighbors are readily easier and more practical due to the **broadcast** nature of ...
Cited by 579 - Related articles - View as HTML - All 29 versions

Route optimization for **mobile** IP
CE Perkins, DB Johnson - Cluster Computing, 1998 - Springer
... Finally, this notification allows any resources con- sumed by the **mobile** node at the previous foreign agent (such as an allocated **radio** channel) to be released imme- diately, rather than waiting for its registration lifetime to expire. ...
Cited by 568 - Related articles - BL Direct - All 6 versions

Random key predistribution schemes for sensor networks
H Chan, A Perrig, D Song - 2003 - computer.org
... The ISM band **radio** receiver communicates at a peak rate of 40Kbps at a range of up to ... and power resources of sensor nodes of- ten makes it undesirable to use **public-key** algorithms, such ... This can be accomplished with a simple local **broadcast** of all key identifiers that a node ...
Cited by 1079 - Related articles - BL Direct - All 49 versions

A quick group key distribution scheme with "entity revocation"

J Anzai, N Matsuzaki, T Matsumoto - Advances in Cryptology- ..., 1999 - Springer
... concept and a concrete scheme of a conference key distribution for secure digital **mobile** communications with ... in section 3. Moreover, we consider that a time-stamp on the **broadcast** data is ... To prevent an attacker from modifying and forging a **public key** on a public bulletin board ...
Cited by 79 - Related articles - BL Direct - All 3 versions

[PDF] An authentication and security protocol for **mobile** computing
Y Zheng - IFIP World Conference on **Mobile** Communications, 1996 - Citeseer
... This section proposes an authentication and key distribution protocol based on a **broadcast** channel in a ... involves a trusted certication authority ca which provides participants of the network, including **mobile** users and base stations, with **public key** certication services. ...
Cited by 37 - Related articles - View as HTML - All 3 versions

Environmental key generation towards clueless agents
J Riordan, B Schneier - **Mobile** Agents and Security, 1998 - Springer
... Unfortunately these techniques are not applicable to **mobile** agents due to the fact that software, unlike hardware, is completely and trivially observable. ... 2. The server returns the **public key**, D , for that time. ... (Again, the server could continuously **broadcast** Ei). ...
Cited by 178 - Related articles - BL Direct - All 14 versions

Cryptology for digital TV **broadcasting**
BM Macq, JJ Quisquater - Proceedings of the IEEE, 1995 - ieeexplore.ieee.org
... in (I), is seen as a **public key** (everyone is able to encrypt) but the key K2, which is ... embeds in his **broadcast** (or, more precisely, in a digital component of his **broadcast**) an entitlement ... to which he is not entitled either by eavesdropping the transmitted signals (**radio** channel, cable ...
Cited by 316 - Related articles - BL Direct - All 4 versions

[PDF] HiperLAN/2–The broadband **radio** transmission technology operating in the 5 GHz freque band
M Johnsson - HiperLAN/2 Global Forum, 1999 - Citeseer
... are bidirectional whereas point-to-multipoint are unidirectional in the direction towards the **Mobile** Terminal ... **Broadcast** and multicast traffic can also be protected by encryption through the use of common keys (all ... one is to use a pre-shared key and the other is to use a **public key**. ...
Cited by 89 - Related articles - View as HTML - All 24 versions

[PDF] Security in public **mobile** communication networks
H Federrath, A Jerichow, D Kesdogan, A ... - WISSENSCHAFTLICHE ..., 1995 - Citeseer
... completely anonymous to the network by delivering the message (possibly end-to-end-encrypted) to all stations (**broadcast**). ... Change of encoding of a message can be implemented using a **public-key** cryptosystem. ... 2.2.1 **Mobile Radio** Systems with Reduced Locating-Ability ...
Cited by 31 - Related articles - View as HTML - BL Direct - All 16 versions

MIXes in **mobile** communication systems: Location management with privacy
H Federrath, A Jerichow, A Pfitzmann - Information Hiding, 1996 - Springer
... The attacker could simply encrypt the outgoing messages of a MIX Mi using its **public key** CMi and ... of the next register (AR1) which, in turn, stores the location information of the **mobile** subscriber. ... P2 to store the LAI and the implicit address TMSI for the **broadcast** message on ...
Cited by 62 - Related articles - BL Direct - All 24 versions

[PDF] Key management for large dynamic groups: One-way function trees and amortized initialization
D Balenson, D McGrew, A Sherman - 1999 - panix.com
... be able to take advantage of efficient **broadcast** channels, such as **radio broadcast** and Internet ... published methods, our algorithm achieves a new low in the required **broadcast** size. ... distributed functionality, they suffer from a linear number of expensive **public-key** operations. ...

Cited by 230 - Related articles - View as HTML - All 13 versions

Toward secure key distribution in truly ad-hoc networks
A Khalili, J Katz, WA Arbaugh - 2003 - computer.org
... exist between devices in the network, or to assume that every principal has a **public-key** certificate which ... We also assume that nodes are **mobile** and that due to this and other environmental conditions ... eg, that all nodes at the time of network formation share a **broadcast** channel ...
Cited by 244 - Related articles - All 12 versions

[PDF] Key establishment in large dynamic groups using one-way function trees
DA McGrew, AT Sherman - Manuscript submitted to IEEE Transactions on ..., 1998 - Citeseer
... be able to take advantage of e cient **broadcast** channels, such as **radio broadcast** and Internet ... 12, 13], require a linear number of **public-key** operations, which are slow in software ... The LKH method 14, 15] achieves logarithmic **broadcast** size, storage, and computational cost. ...
Cited by 293 - Related articles - View as HTML - All 12 versions

Conference key distribution schemes for secure digital **mobile** communications
MS Hwang, WP Yang - IEEE Journal on Selected areas in ..., 1995 - ieeexplore.ieee.org
... 111. Two NEW EFFICIENT SCHEMES In this section we present two conference key distribution protocols for digital **mobile** communications. The first is based on **public-key** cryptography. In this scheme, the network center need not keep the secret keys of all conferees. ...
Cited by 40 - Related articles - BL Direct - All 3 versions

[PDF] Preserving privacy in a network of **mobile** computers
DA Cooper, KP Birman - IEEE Symposium on Security and Privacy, 1995 - Citeseer
... An example of a **public key** scheme is RSA 18]. As with most public ... Since messages are **broadcast** to every computer, recipient anonymity is also guaranteed. ... This technique is also not well suited for **mobile** computers which may frequently dis- connect from the network. ...
Cited by 90 - Related articles - View as HTML - BL Direct - All 22 versions

A key-management scheme for distributed sensor networks
L Eschenauer, VD Gligor - Proceedings of the 9th ACM Conference ..., 2002 - portal.acm.org
... of the network, and control nodes, which monitor the status of and **broadcast** simple commands ... have limited, if any, mobility after deployment, some nodes are highly **mobile** (eg, data ... nodes in this range make it impractical to use typical asymmetric (**public-key**) cryptosystems to ...
Cited by 2014 - Related articles - All 53 versions

Key-insulated **public key** cryptosystems
Y Dodis, J Katz, S Xu, M Yung - Advances in Cryptology—EUROCRYPT ..., 2002 - Springer
... Cryptographic computations (decryption, signature genera- tion, etc.) are often performed on a relatively insecure device (eg, a **mobile** device or an Internet-connected ... All cryptographic computations are still done on the insecure device, and the **public key** remains unchanged. ...
Cited by 197 - Related articles - BL Direct - All 16 versions

[PDF] **Public key** protocols for wireless communications
C Boyd, DG Park - Proceedings of the 1st International Conference on ..., 1998 - Citeseer
... As for A's way to get the **public key** of the network, it may receive the key value from the system **broadcast** channel of ... B can get the **public key** of the user from the certificate data of A if it is included inside the ... Note that the first message can be pre-calculated off-line by the **mobile**. ...
Cited by 45 - Related articles - View as HTML - All 10 versions

[PDF] Location management strategies increasing privacy in **mobile** communication
D Kesdogan, H Federrath, A Jerichow, A ... - 12th International ..., 1996 - Citeseer
... For the reachability of a **mobile** subscriber signaling takes place in more than one LA. ... Another difference to GSM is the necessary bandwidth on the **broadcast** channel for signaling. By using

public key cryptography, one paging message is approximately 500 bit long. ...
Cited by 31 - Related articles - View as HTML - All 22 versions

[PDF] Efficient distribution of key chain commitments for **broadcast** authentication in distributed sensor networks
D Liu, P Ning. . - Proceedings of the 10th Annual Network and ..., 2003 - Citeseer
... networks. Gen- erally, an asymmetric mechanism, such as **public key** cryptography, is required to authenticate **broadcast** messages. Otherwise, a malicious receiver can easily forge any packet from the sender. However, due to the ...
Cited by 183 - Related articles - View as HTML - All 20 versions

[PDF] Design issues in **mobile**-agent programming systems
NM Karnik, AR Tripathi - IEEE concurrency, 1998 - Citeseer
... be integrated with the name resolution service, so that a name lookup can return a **public key** in addition ... Table 2 summarizes the basic mobility support provided by the seven **mobile** agent systems surveyed ... Another model is to provide **broadcast** of events to all agents in a group ...
Cited by 288 - Related articles - View as HTML - BL Direct - All 13 versions

Proxy-based security protocols in networked **mobile** devices
M Burnside, D Clarke, T Mills, A Maywah, S ... - Proceedings of the ..., 2002 - portal.acm.org
... Devices themselves may be **mobile** and may change loca- tions. ... At the same time that this information is **broadcast** in the I~F spectrum, the beacon also ... 4. PROXY TO PROXY PROTOCOL SPKI/SDSI (Simple **Public Key** Infrastructure/Simple Dis- tributed Security Infrastructure) [7 ...
Cited by 75 - Related articles - All 29 versions

SEAD: Secure efficient distance vector routing for **mobile** wireless ad hoc networks
YC Hu, DB Johnson, A Perrig - Ad Hoc Networks, 2003 - Elsevier
... that can create routing loops are more common in wireless and **mobile** networks such ... trust relationships from PGP-like certificates without relying on a trusted **public key** infrastructure [19]. ... Any efficient **broadcast** authentication mechanism, such as TESLA [37], HORS [42], or TIK ...
Cited by 852 - Related articles - All 52 versions

Mitigating routing misbehavior in **mobile** ad hoc networks
S Marti, TJ Giuli, K Lai, M Baker - ... International conference on Mobile ..., 2000 - portal.acm.org
... One advantage of wireless is the ability to transmit data among users in a common area while remaining **mobile**. ... not have this information (for instance if it were implemented on top of a hop-by-hop routing protocol), then a malicious or broken node could **broadcast** the packet to ...
Cited by 1885 - Related articles - All 75 versions

[PDF] MOCA: **Mobile** certificate authority for wireless ad hoc networks
S Yi, R Kravets - 2nd Annual PKI Research Workshop Pre-Proceedings, 2003 - Citeseer
... PKI (**Public Key** Infrastructure), an infrastructure for managing digital certificates, was introduced exactly for ... operator chooses MOCAs based on an observation of heterogeneity among **mobile** nodes, typically ... a certification service cheaply by using a one-hop **broadcast** for the ...
Cited by 226 - Related articles - View as HTML - All 30 versions

Authenticated ad hoc routing at the link layer for **mobile** systems
J Binkley, W Trost - Wireless Networks, 2001 - Springer
... In the ad hoc protocol, all communicants **broadcast** beacons, not just **Mobile**-IP agents. ... registration packet could include the authenticated addressing information and the **mobile** node would ... The symmetric keys might be replaced with **public key** cryptography [6]. Portland State ...
Cited by 53 - Related articles - BL Direct - All 22 versions

The first ten years of **public-key** cryptography
W Diffie - Proceedings of the IEEE, 1988 - ieeexplore.ieee.org

Page 1. The First Ten Years of **Public-Key** Cryptography ... Hoffman wanted term papers and required each student to submit a proposal early in the term. Merkle addressed the problemof **public-key** distributionoras hecalled it"Secure Communication over Insecure Channels" [70]. ...
Cited by 193 - Related articles - All 13 versions

[PDF] A novel authentication scheme for ad hoc networks
L Venkatraman, DP Agrawal - IEEE Wireless Communications and ..., 2000 - Citeseer
... purview. The CA ought to be a completely trusted entity and issues a digi- tal certificate to any **mobile** host that needs to be authen- ticated. ... members. This key is encrypted with the system **public key** and **broadcast** by the head. Each ...
Cited by 73 - Related articles - View as HTML - All 9 versions

Business models and transactions in **mobile** electronic commerce: requirements and properties
A Tsalgatidou, E Pitoura - Computer Networks, 2001 - Elsevier
... If used, eg, to **broadcast** multimedia contents over the network, the network would collapse, because ... is charged per connection-time, while for others (eg, in packet **radio**), it is ... of tariffs, eg, session-based, transaction-based, connection time-based, while in **mobile** e-commerce ...
Cited by 133 - Related articles - All 15 versions

Multicast security and its extension to a **mobile** environment
L Gong, N Shacham - Wireless Networks, 1995 - portal.acm.org
... We also describe an initial architectural design for secure multicast in a **mobile** environment. We conclude Wireless Networks 1 (1995) 281^295 281 ... the order of O(2n). The problem we examine here is how to securely **broadcast** a message when **public-key** sys- tems ...
Cited by 47 - Related articles - All 7 versions

SPINS: Security protocols for sensor networks
A Perrig, R Szewczyk, JD Tygar, V Wen, DE ... - Wireless networks, 2002 - portal.acm.org
... Keywords: secure communication protocols, sensor networks, **mobile** ad hoc networks, MANET ... and developing µTESLA (the "micro" version of TESLA), providing authenticated streaming **broadcast**. ... bytes RAM 512 bytes EEPROM Communication 916 MHz **radio** Bandwidth 10 ...
Cited by 2260 - Related articles - BL Direct - All 163 versions

Dynamic participation in a secure conference scheme for **mobile** communications
MS Hwang - IEEE transactions on vehicular technology, 1999 - ieeexplore.ieee.org
... 4], and it is suitable to distribute CK over a public **broadcast** channel. ... T. Okamoto, and S. Tsujii, "On key distri- bution and authentication in **mobile radio** networks," in ... A. Shamir, and L. Adleman, "A method for obtaining digital signatures and **public key** cryptosystems," Commun. ...
Cited by 48 - Related articles - BL Direct - All 5 versions

Making the key agreement protocol in **mobile** ad hoc network more efficient
G Yao, K Ren, F Bao, R Deng, D Feng - Applied Cryptography and ..., 2003 - Springer
... To securely **broadcast** a message, all the members in the network need share a ... encryption algorithms (such as DES, AES) is much faster than the **public key** based protocols ... Among the **mobile** nodes, backbone nodes have an additional powerful **radio** to establish wireless links ...
Cited by 19 - Related articles - BL Direct - All 6 versions

Proactive secret sharing or: How to cope with perpetual leakage
A Herzberg, S Jarecki, H Krawczyk, M Yung - Advances in Cryptology— ..., 1995 - Springer
... phase the servers hold new shares of the secret t . THE **MOBILE** ADVERSARY MODEL. ... We mume also that the adversary is connected to the **broadcast** channel C, which ... underlying cryptographic primitives on which we bsse our design (this includes **public-key** encryption and ...
Cited by 461 - Related articles - BL Direct - All 8 versions

Networks without user observability* 1

A Pfitzmann, M Waidner - Computers & Security, 1987 - Elsevier
... a " transmission on demand basis" even for the classical **broadcast** services TV and **radio**, major parts ... be made completely anonymous to the network by delivering the message to all stations (**broadcast**). ... Invisible implicit addresses can be realized with a **public key** cryptosystem ...
Cited by 224 - Related articles - All 8 versions

Techniques for Privacv and Authentication in &son a I Com mun ication Systems
D Brown - IEEE Personal Communications, 1995 - ieeexplore.ieee.org
... GSM systems have dealt with this problem by the practice of using "temporary **mobile** station identities" (tmsi). ... The hybrid method offers some protocol advantages as well. Since the Access Controller's **public key** is **broadcast**, a registration can be anonymous. ...
Cited by 70 - Related articles - All 6 versions

Securing ad hoc networks
L Zhou, ZJ Haas - IEEE network, 1999 - ieeexplore.ieee.org
... failures, such as **radio** propagation impairment, or hccausc of malicious attacks on the network. ... Unlike other wirelcss **mobile** networks, soch as mohile IP 1, nodes in an ad hoc network may ... The CA has a publicIpri- vatc kcy pair, wilh its **public key** known to evcry node, and signs ...
Cited by 1893 - Related articles - BL Direct - All 87 versions

Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its **public key** infrastructure integration
CF Grecas, SI Maniatis, IS Venieris - Mobile Networks and Applications, 2003 - Springer
... entire network facilitates as well the distribution of the pub- lic key in the case of **mobile** network interconnections ... sends the Identity Message to the MSC/VLR with its identity data, using the VLR's **public key**, see figure 3, possibly emitted on the **Broadcast** Channel (BCH ...
Cited by 29 - Related articles - BL Direct - All 4 versions

A new set of passive routing attacks in **mobile** ad hoc networks
J Kong, X Hong, M Gerla - IEEE Military Communications ..., 2003 - ieeexplore.ieee.org
... imprac- tical conjecture if we assume data packets transmitted in wireless **broadcast** channel are ... Legitimate network members can employ **public key** cryptosystems (eg, RSA, El Gamal) and symmetric key ... collaborative adver- saries to trace the motion pattern of a **mobile** node. ...
Cited by 26 - Related articles - BL Direct - All 12 versions

Cryptographic solution to a problem of access control in a hierarchy
SG Akl, PD Taylor - ACM Transactions on Computer Systems (..., 1983 - portal.acm.org
... controls; information flow controls; E.3 [Data]: Data En- cryption--Data Encryption Standard (DES); **public-key** cryptosystems ... to files that are stored in a central computer memory, but also to messages **broadcast** on a communication network using telephone lines or **radio** waves ...
Cited by 337 - Related articles - All 2 versions

[PDF] Challenges in **mobile** electronic commerce
A Tsalgatidou, J Veijalainen, E Pitoura - Proceeding of IeC, 2000 - Citeseer
... **Broadcasting** offers an efficient means to disseminate information to a large consumer population. ... For example, if a customer buys a product through its **mobile** phone, this ... Techniques like the asymmetric cryptographic algorithm (also called **Public Key** algorithm) are used to ...
Cited by 46 - Related articles - View as HTML - All 9 versions

[PDF] Sprite: A simple, cheat-proof, credit-based system for **mobile** ad-hoc networks
S Zhong, J Chen, YR Yang - IEEE INFOCOM, 2003 - Citeseer
... where PK0 is the **public key** of the sender. ... As route-discovery **broadcast** can be viewed as a special case of multicast, this approach can also be applied to multicast if ... In the evaluations below, our **mobile** node is a Laptop with an Intel **Mobile** Pentium III processor at 866MHz. ...
Cited by 671 - Related articles - View as HTML - BL Direct - All 34 versions

MANETconf: Configuration of hosts in a **mobile** ad hoc network
S Nesargi, R Prakash - ... -First Annual Joint Conference of the ..., 2002 - ieeexplore.ieee.org
... I. I NTRODUCTION A **mobile** ad hoc network (MANET) is a group of **mobile**, wireless nodes which cooperatively and spontaneously form an IP-based network. ... If there is any response that, too, is multi- cast/**broadcast** on the same link. ...
Cited by 328 - Related articles - BL Direct - All 25 versions

Key agreement in ad hoc networks* 1
N Asokan, P Ginzboorg - Computer Communications, 2000 - Elsevier
... These **public key** certificates can allow participants to verify the binding between the IP addresses and keys ... The strongest attacker can disrupt any protocol by jamming the **radio** channel or modifying ... The leader will **broadcast** the message in step 1. The rest of the messages will ...
Cited by 408 - Related articles - All 11 versions

[PDF] Trust management and proof-carrying code in secure **mobile**-code applications
J Feigenbaum, P Lee - ... Workshop on Foundations for Secure Mobile ..., 1997 - Citeseer
... A may require metadata signed by C that provides a valid **public key** for B, a ... This would be accomplished by enclosing fragments of **mobile** code into each network packet, to ... networks seem to provide a means for better support multicast and **broadcast** applications, essentially ...
Cited by 35 - Related articles - View as HTML - All 21 versions

Weak duplicate address detection in **mobile** ad hoc networks
NH Vaidya - ... international symposium on Mobile ad hoc networking ..., 2002 - portal.acm.org
... to the Address Resolution Protocol (ARP), such that ARP replies are sent by a **broadcast**, as opposed ... This paper considers the problem of duplicate address de- tection (DAD) in **mobile** ad hoc networks. ... and it may not be possible to embed the key 3 If **public-key** cryptography is ...
Cited by 248 - Related articles - All 27 versions

Strategies for enhancing routing security in protocols for **mobile** ad hoc networks* 1
L Venkatraman, DP Agrawal - Journal of Parallel and Distributed ..., 2003 - Elsevier
... Moreover, this authority can be well protected since it is not **mobile** like the other nodes. ... has elapsed, and if the node mobility are relatively high, each node might need to store the **public key** of large ... Denial of service: This can be done by generating false **broadcast** packets like ...
Cited by 48 - Related articles - BL Direct - All 6 versions

An optimized protocol for **mobile** network authentication and security
X Yi, E Okamoto, KY Lam - ... Mobile Computing and Communications ..., 1998 - portal.acm.org
... tention as it represents one of the earliest solution employ- ing a combination of both private-key and **public-key** encryp- tion. ... In the same article, Zheng proposed an authentication and key distribution protocol that utilized a **broadcast** channel for a **mobile** user authenticating ...
Cited by 15 - Related articles - All 3 versions

LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks
S Zhu, S Xu, S Setia, S Jajodia - 2003 - computer.org
... steps in which a control packet, eg, a route request packet, is **broadcast** to all ... Further, the resources of a **mobile** node such as battery power, computational capacity and bandwidth ... Third, we assume each node has a **public key** certificate signed by a trusted certificate authority ...
Cited by 61 - Related articles - All 18 versions

[PDF] Security issues in a future vehicular network
M El Zarki, S Mehrotra, G Tsudik, N ... - European Wireless, 2002 - Citeseer
... Also, vehicles communicating in an ad hoc network **broadcast** their data, thus, pair-wise (or group-wise) key distribution is ... issues: a related concern in many **mobile** networks is the low CPU speed of the **mobile** node. ... Certification Infrastructure (PKI): **public key** digital signatures ...
Cited by 90 - Related articles - View as HTML - All 9 versions

A new anonymous conference key distribution system based on the elliptic curve discrete logar problem* 1
CC Yang, TY Chang, MS Hwang - Computer Standards & Interfaces, 2003 - Elsevier
... 3. M.-S. Hwang and WP Yang, Conference key distribution protocols for digital **mobile** communication systems. ... 194–202. 8. CH Lin, CC Chang and RCT Lee, A conference key **broadcasting** system using sealed lock. ... 9. A. Menezes, Elliptic Curve **Public Key** Cryptosystem. ...
Cited by 24 - Related articles - All 7 versions

[PDF] **Mobile** ad hoc networking: imperatives and challenges
I Chlamtac, M Conti, JJN Liu - Ad Hoc Networks, 2003 - Citeseer
... networking applications can be traced back to the DARPA Packet **Radio** Network (PRNet ... and store- and-forward routing, and its possible application in **mobile** wireless environment. PRNet features a distributed architecture consisting of network of **broadcast** radios with minimal ...
Cited by 556 - Related articles - View as HTML - All 34 versions

[PDF] Ubibay: An auction system for **mobile** multihop ad-hoc networks
H Frey, JK Lehnert, P Sturm - Workshop on Ad hoc Communications and ..., 2002 - Citeseer
... to redundant rebroadcasts, contention and packet collisions, also known as the **broadcast** storm problem ... might be reduced by using the knowledge about temporary adjacent **mobile** devices as ... In [9] al- gorithms for a self-organized **public-key** infrastructure are presented, where ...
Cited by 16 - Related articles - View as HTML - All 18 versions

[PDF] A streaming architecture for next generation internet
A Dutta, H Schulzrinne - Proc. of ICC'01, 2001 - Citeseer
... of bringing quality audio/video **broadcast** to the people in remote site, and to the wireless clients who are **mobile**. ... stream should effectively prevent IMCs, as well as the non-paid RASs, from receiving the **broadcast** content. ... **Public key** technology is em- ployed for this purpose. ...
Cited by 13 - Related articles - View as HTML - All 9 versions

[PDF] Securing **mobile** ad hoc networks
P Papadimitratos, ZJ Haas - The handbook of ad hoc wireless networks, 2003 - Citeseer
... A second proposal to secure AODV makes use of **public key** cryptography as well and ... The Secure Routing Protocol The Secure Routing Protocol (SRP) [17] for **mobile** ad hoc ... Communication takes place over a **broadcast** medium, and it is assumed that malicious nodes, which ...
Cited by 39 - Related articles - View as HTML - All 9 versions

[PDF] Energy-efficient and low-latency key management for sensor networks
DW Carman, BJ Matt, GH Cirincione - ... Security Research Journal, 2003 - isso.sparta.com
... recent investigation in establishing keys to secure link-layer broadcasts for a prototype Army sensor network **radio** reveals that ... other members Uni-cast to a single member 1 6 5 4 3 2 Group leader **broadcast** its certificate (and its ephemeral **public key**) Group members ...
Cited by 38 - Related articles - View as HTML - All 3 versions

Generalization of M **Public Key** System and Analysis of Its Performance on Noisy Channel [J]
W Xin-mei - Acta Electronica Sinica, 1986 - en.cnki.com.cn
... A JOINT SIGNATURE ENCRYPTION AND ERROR CORRECTION **PUBLIC-KEY** CRYPTOSYSTEM BASED ... University,Dalian,Liaoning 116026,China 2.National **Mobile** Communications Research ... Tzeng(Xidian University, Xian) (Lehigh Univ.);**Broadcast** ...
Cited by 9 - Related articles - Cached

[PDF] Preventing selfishness in open **mobile** ad hoc networks
H Miranda, L Rodrigues - Proc. Seventh CaberNet Radicals Workshop, 2002 - Citeseer
... However, there is a significant difference between the fixed and the **mobile** environment. ... The modules use a **Public Key** Infrastructure (PKI) to ensure the authentication of the tamper ... by being suspicious on the incoming selfish- ness alerts that other nodes **broadcast** and relying ...

Cited by 35 - Related articles - View as HTML - All 9 versions

Secure multicast in wireless networks of **mobile** hosts: protocols and issues
D Bruschi, E Rosti - **Mobile** Networks and Applications, 2002 - Springer
... Msi ⊆ M is the set of **mobile** hosts in the cell con- trolled by support station si. ... metric key pair associated with entity j in the PKI, where pj is the **public key** and p −1 j is the private ... or a group of senders/receivers, eg, a subset of S or of M, in case of multicast or **broadcast** messages ...
Cited by 59 - Related articles - BL Direct - All 6 versions

[PDF] An infrastructure for distributed and dynamic network management based on **mobile** agei technology
D Gavalas, M Ghanbari, M O'Mahony, D ... - IEEE International ..., 1999 - Citeseer
... **Broadcast** the bytecode to all the active agents Yes No ... "Infrastructure for Advanced Network Management based on **Mobile** Code", Proceedings of ... [9] Rivest RL, Shamir A., Adleman L., "A Method for obtaining Digital Signatures and **Public-Key** Cryptosystems", Communication ...
Cited by 55 - Related articles - View as HTML - BL Direct - All 5 versions

Efficient Dynamic-Resharing "Verifiable Secret Sharing" Against **Mobile** Adversary
N Alon, Z Galil, M Yung - Algorithms—ESA'95, 1995 - Springer
... The second method is a direct (and efficient) but requires, in addition to **public key** system, homornorphic ... linear faults (say, n/3 faults which are the upper bound for, say, **broadcast** or agreement ... on corrupted trustees within a time period, but lets the adversary be **mobile** and be ...
Cited by 23 - Related articles - BL Direct - All 9 versions

Coding constructions for blacklisting problems without computational assumptions
R Kumar, S Rajagopalan, A Saha - Advances in Cryptology—Crypto'99, 1999 - Springer
... cast channels these devices could function by means of preset one-time pads, while for analog **broadcast** channels (such as **radio** or cable ... could function using private-key encryption, or using **public-key** encryption.1 In this framework, to solve **broadcast** security problems ...
Cited by 116 - Related articles - BL Direct - All 15 versions

[PDF] Analysis of security and privacy in **mobile** IP
A Fasbender, D Kesdogan, O Kubitz - 4th International Conference on ..., 1996 - Citeseer
... is no expectation of guaranteed privacy in cellular telephone networks, which **broadcast** their signals ... recommends that if absolute protection from traffic analysis is required, the **mobile** node can ... the help of so-called mixes is a technique based on **public key** cryptography mainly ...
Cited by 46 - Related articles - View as HTML - All 8 versions

A practical and secure fault-tolerant conference-key agreement protocol
WG Tzeng - **Public Key** Cryptography, 2000 - Springer
... to establish a com- mon conference key K such that all their communications thereafter are encrypted with the key K. In this paper we propose a practical and prov- ably secure fault-tolerant conference-key agreement protocol under the authenticated **broadcast** channel model. ...
Cited by 37 - Related articles - BL Direct - All 5 versions

New multiparty authentication services and key agreement protocols
G Ateniese, M Steiner, G Tsudik - IEEE Journal on Selected ..., 2000 - ieeexplore.ieee.org
... How- ever, there are some important assumptions underlying this pro- tocol. Specifically, it requires each to **broadcast** to the rest of the group and to receive messages in a single round. Moreover ... corre- sponding long-term **public key** of . ...
Cited by 287 - Related articles - BL Direct - All 22 versions

Key establishment in large dynamic groups using one-way function trees
AT Sherman, DA McGrew - IEEE transactions on Software ..., 2003 - computer.org
... Furthermore, the basic unit of cost for all GDH methods includes **public-key** operations, which

are slow in software ... type of "out-of-band" resynchronization for users who have lost contact with the **broadcast** signal, as might happen when an airplane flies out of **radio** range. ...
Cited by 190 - Related articles - BL Direct - All 11 versions

Anonymous channel and authentication in wireless communications
WS Juang, CL Lei, CY Chang - Computer communications, 1999 - Elsevier
... Due to the roaming, dynamic channel assignment and **broadcasting** features of **mobile** communications, if a ... Y. Also, let K vh be the secret key shared by H and V, HID be H's identification number, {m} e r denote the ciphertext of m encrypted using Rabin's **public key** e r ...
Cited by 59 - Related articles - All 9 versions

Protecting a **mobile** agent's route against collusions
D Westhoff, M Schneider, C Unger, F ... - Selected Areas in ..., 2000 - Springer
... its relevant signature and all the remaining ciphertext by using its private key di that corresponds to the **public key** ei. ... Protecting a **Mobile** Agent's Route against Collusions 221 ... For example, a malicious working context ci can **broadcast** to all its accomplices that it was visited by a ...
Cited by 30 - Related articles - BL Direct - All 5 versions

Information-theoretically secure secret-key agreement by NOT authenticated public discussion
U Maurer - Proceedings of the 16th annual international ..., 1997 - portal.acm.org
... Corollary 2. A **public-key** cryptosystem can be computationally secure but not information-theoretically (Le ... one discussed below in which Alice, Bob, and Eve receive noisy versions of a random string **broadcast** by a satellite or of the signal emitted by a deep space **radio** source ...
Cited by 47 - Related articles - BL Direct - All 17 versions

Public-key support for group collaboration
C Ellison, S Dohrmann - ACM Transactions on Information and ..., 2003 - portal.acm.org
... that we address and that we see in our daily lives is on **mobile** machines, often ... whether the member is connected and, if so, its network address and its **public key**) would be ... 802.11 ad hoc mode, in NGC implementations so far), presence information is gathered by **broadcast**. ...
Cited by 32 - Related articles - All 2 versions

Secure **mobile** agents on ad hoc wireless networks
E Sultanik, D Artz, G Anderson, M Kam, W Regli ... - The Fifteenth Innovative ..., 2003 - aaai.org
... The security framework uses a combination of symmetric and **public-key** cryptography to support encrypted ... state; make deci- sions about their itineraries (ie, if they are **mobile** agents) based on ... may not mirror the connectivity of the network— hence, a **broadcast** message from ...
Cited by 30 - Related articles - All 9 versions

Effects of power conservation, wireless coverage and cooperation on data dissemination amon **mobile** devices
M Papadopouli, H Schulzrinne - ... international symposium on Mobile ..., 2001 - portal.acm.org
... and the destina- tion are required to have PGP in order to encrypt (using the **public key**) and then ... its destination with a constant speed uniformly selected from (0m/s,1.5m/s). When a **mobile** host reaches ... The **broadcast** is scheduled at a random time selected from the on interval. ...
Cited by 231 - Related articles - All 33 versions

An authentication framework for hierarchical ad hoc sensor networks
M Bohge, W Trappe - Proceedings of the 2nd ACM workshop on ..., 2003 - portal.acm.org
... nodes that relay information from sensor nodes to ac- cess points, and (D) low-powered **mobile** sensor nodes ... system for low-powered devices, we need a certificate structure that does not employ **public key** cryptography. TESLA [12] is a **broadcast** authentication technique that ...
Cited by 97 - Related articles - All 20 versions

Towards flexible credential verification in **mobile** ad-hoc networks

SL Keoh, E Lupu - ... international workshop on Principles of **mobile** ..., 2002 - portal.acm.org
... Note that since all the credentials in a CAS may be confirmed by assertions from the same source and since the recipient has the **public key** of the ... In order to enhance the revocation capabilities in **mobile** ad-hoc network, issuers of ASSs may choose to **broadcast** to peers ...
Cited by 21 - Related articles - All 10 versions

Mobile agent middleware for **mobile** computing
P Bellavista, A Corradi, C Stefanelli - Computer, 2001 - ieeexplore.ieee.org
... 8,9 For example, many MA sys- tems integrate with **public key** infrastructures, sim- plifying ... to the limit because it should intervene at any migration and at any **mobile** entity search. ... scale without requiring specific knowledge; a client typically requests the service with a **broadcast** ...
Cited by 174 - Related articles - BL Direct - All 5 versions

[PDF] Security and privacy in **radio**-frequency identification devices
SA Weis - 2003 - Citeseer
... Page 20. Fundamentally, readers are quite simple devices and could be incorporated into **mobile** ... a narrow band of **radio** frequencies specified by regulation agencies such as the Federal ... the collision. The reader will then **broadcast** a bit indicating whether tags who **broadcast** ...
Cited by 262 - Related articles - View as HTML - All 26 versions

[PDF] Cooperative routing in **mobile** ad-hoc networks: Current efforts against malice and selfish
S Buchegger, JY Le Boudec - Lecture Notes on Informatics, Mobile ..., 2002 - Citeseer
... wireless links are vulnerable to jamming and by their inherent **broadcast** nature facilitate ... refreshing for distributed certification authorities for key management in **mobile** ad-hoc ... Localized certification based on the **public key** infrastructure (PKI) with certification- authority and ...
Cited by 36 - Related articles - View as HTML - All 18 versions

Protocols using anonymous connections: **Mobile** applications
M Reed, P Syverson, D Goldschlag - Security Protocols, 1998 - Springer
... of one way communication, a means to guarantee that only the responder can receive the message, eg, **public key** encryption ... cost of **broadcast**. ... Other approaches to anonymity in **mobile** phone systems occur in [2] and [3]. Another approach to private location tracking occurs in [7 ...
Cited by 27 - Related articles - BL Direct - All 29 versions

Anonymous conference key distribution systems based on the discrete logarithm problem
YM Tseng, JK Jan - Computer Communications, 1999 - Elsevier
... Hellman scheme [1], the system assigns a secret key x i Z q * and computes the **public key** y i ... 4. MS Hwang and WP Yang, Conference key distribution schemes for secure digital **mobile** communications ... 5. T. Hwang and JL Chen, Identity-based conference key **broadcast** systems ...
Cited by 24 - Related articles - All 5 versions

[PDF] A secure routing protocol for ad hoc networks
B Dahill, BN Levine, E Royer, C Shields - ..., Tech. Rep. UM-CS-2001-037, 2001 - scss.tcd.ie
... Additionally, **mobile** nodes in the managed-open environment reside within some com- mon context or geographic proximity ... signed by T . All nodes must maintain fresh certificates with the trusted server and must know T 's **public key**. ... A → **broadcast** : [RDp, IpK, certa, Na, t]Ka- (2 ...
Cited by 254 - Related articles - View as HTML - All 11 versions

A wireless public access infrastructure for supporting **mobile** context-aware IPv6 applications
A Friday, M Wu, S Schmid, J Finney, K ... - ... on Wireless **mobile** ..., 2001 - portal.acm.org
... The **broadcast** protocol is one of the key mechanisms for promoting the scalability of GUIDE ... In **Mobile** IPv6 this limitation implies that a potential attacker must remain co-located with ... impersonation of the authentication server, the payload is encrypted using the **public key** of the ...
Cited by 10 - Related articles - All 10 versions

[PDF] **Mobile** agents and security
MS Greenberg, JC Byington, DG Harper - IEEE Communications Magazine, 1998 - ic.uff.br
... The recipi- ents of this **broadcast** include the auto-configuration server on β and the two malicious **mobile** ... Authenticating Credentials — A **mobile** agent is digitally signed by one or more parties using one of a number of algo- rithms, such as a **public key** signature algorithm ...
Cited by 175 - Related articles - View as HTML - BL Direct - All 4 versions

Friends and foes: Preventing selfishness in open **mobile** ad hoc networks
H Miranda, L Rodrigues - 23rd International Conference on ..., 2003 - ieeexplore.ieee.org
... Some resources, like battery power, are scarce in a **mobile** environment and can be depleted at ... To ensure the authentication of the tamper resistant modules, a **Public Key** Infrastructure (PKI) is used ... DSR, multi-hop routes can be learned either by the replies to the **broadcast** of a ...
Cited by 28 - Related articles - All 8 versions

Mobile peer membership management to support multimedia streaming
SS Kang, MW Mutka - 23rd International Conference on ..., 2003 - ieeexplore.ieee.org
... When a **mobile** device is ready to connect to an outside network via its ISP, it ... a single-member CHUM network, and becomes a proxy that will periodically **broadcast** a service ... Packet Length Packet Type Packet Type Packet Length Session Key **Public Key** Random ID Session ID ...
Cited by 7 - Related articles - All 14 versions

New directions in cryptography
W Diffie, M Hellman - IEEE Transactions on information ..., 1976 - ieeexplore.ieee.org
... person can originate messages but many people can receive messages, this can be viewed as a **broadcast** cipher. ... Some partial solutions are given, and it is shown how any **public key** cryptosystem can be transformed into a one ... In **radio**, by comparison, the situation is re- versed ...
Cited by 7998 - Related articles - All 154 versions

[PDF] Achieving user privacy in **mobile** networks
B Askwith, M Merabti, Q Shi, K Whiteley - proceedings of the 13th ..., 1997 - ece.umd.edu
... can then decrypt the message (leaving the message encrypted only under y's **public key**) and send it ... using random detours within mix routes, making replies anonymous for **broadcast** messages, and ... Although [21] is not directed at **mobile** networks it does offer some interesting ...
Cited by 26 - Related articles - View as HTML - All 7 versions

Secure aggregation for wireless networks
L Hu, D Evans - 2003 Symposium on Applications and the ..., 2003 - ieeexplore.ieee.org
... [1] present a solution to complete an authenticated key exchange protocol over the wireless link without a **public key** infrastructure, but it ... We design our protocol around these assumptions: 1. The base station is powerful and can **broadcast** messages to all nodes directly. ...
Cited by 240 - Related articles - All 21 versions

Chinese lotto as an exhaustive code-breaking machine
JJ Quisquater, YG Desmedt - COMPUTER,, 1991 - computer.org
... In **public-key** cryptosystems, where K # K', we call K the **public key** and K'the secret decryption key; pub- lishing K does not endanger the security of the cryptosystem. ... A plaintext-ciphertext pair is **broadcast** regularly by all **radio** and television sta- tions. ...
Cited by 22 - Related articles - All 5 versions

The design and implementation of a private message service for **mobile** computers
DA Cooper, KP Birman - Wireless Networks, 1995 - portal.acm.org
... As with most **public key** encryption schemes, RSA can also be used to sign messages. ... Since messages are **broadcast** to every computer, recipient anonymity is also guaran- ... This techni- que is also not well suited for **mobile** computers which may frequently disconnect from the ...
Cited by 17 - Related articles - All 10 versions

Create email alert

Gooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10 Next

"public key" broadcast (mobile OR ra Search

Go to Google Home - About Google - About Google Scholar